AO 93 (Rev. 12/09) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the
District of Arizona

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* GMC Savana U-Haul van bearing Arizona License Plate AL82438, at 529 W. 32nd Street, Yuma, AZ 85364	)	Case No. 23-3002 MB

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the _____ District of Arizona
(identify the person or describe the property to be searched and give its location):
See Attachment A, incorporated by reference

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:
See Attachment B, incorporated by reference

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before 1-14-23
(not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10 p.m. ☑ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge on duty in the District of Arizona .
(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)* ☐ for _____ days *(not to exceed 30)*.
☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 12-31-22 @ 10:55 p.m. M Morrissey
Judge's signature

City and state: Phoenix, Arizona Michael T. Morrissey, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

Property to Be Searched

The vehicle is a white GMC Savana U-Haul van bearing Arizona License Plate AL82438, Vehicle Identification Number (VIN): 1GTW7AFPXN1247737, currently parked at *Cal-Ranch,* 529 W. 32nd Street Yuma, AZ 85364.

ATTACHMENT B

Property to be seized

1. Firearms, ammunition, magazines, cases, boxes, holsters, slings, gun pieces, gun cleaning items or kits, ammunition belts, original box packaging, targets, expended pieces of lead, and records, receipts, or other paperwork showing the purchase, storage, disposition, or dominion and control over firearms and ammunition;

2. Records, receipts, notes, ledgers, customer lists, invoices, and any other documentation related to the manufacture, importation, transportation, ordering, purchase, sale, or distribution of firearms;

3. Records relating to the receipt, transportation, deposit, transfer, or distribution of money, including but not limited to, direct deposit confirmations, wire transfers, money orders, cashier's checks, check stubs, PayPal or other electronic money transfer services, check or money order purchase receipts, account statements, and any other records reflecting the receipt, deposit, or transfer of money;

4. Safe deposit box keys, storage locker keys, safes, and related secure storage devices, and documents relating to the rental or ownership of such units;

5. Indicia of occupancy, residency, rental, ownership, or use of the Subject Premises and Vehicle found thereon during the execution of the warrant, including, utility and telephone bills, canceled envelopes, rental, purchase or lease agreements, identification documents, keys, records of real estate transactions, vehicle titles and registration, and vehicle maintenance records;

6. Cellular Phones (known as "electronic storage media");

7. Records evidencing ownership or use of electronic storage media, including sales receipts, registration records, and records of payment;

8. Any records and information found within the digital contents of any

electronic storage media seized from the Subject Premises, including:

a. all information related to the sale, purchase, receipt, shipping, importation, transportation, transfer, possession, or use of weapons and/or controlled substances;

b. all information related to buyers or sources of weapons and/or controlled substances (including names, addresses, telephone numbers, locations, or any other identifying information);

c. all bank records, checks, credit card bills, account information, or other financial records;

d. all information regarding the receipt, transfer, possession, transportation, or use of firearm proceeds;

e. any information recording schedule or travel;

f. evidence of who used, owned, or controlled the electronic storage media at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, correspondence, and phonebooks;

g. evidence indicating how and when the electronic storage media were accessed or used to determine the chronological context of electronic storage media access, use, and events relating to crime under investigation and to the electronic storage media user;

h. evidence indicating the electronic storage media user's state of mind as it relates to the crime under investigation;

i. evidence of the attachment to an electronic storage medium of another storage device or similar container for electronic evidence;

j. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the electronic storage media;

k. evidence of the times the electronic storage media were used;

l. passwords, encryption keys, and other access devices that may be necessary to access the electronic storage media;

m. documentation and manuals that may be necessary to access the electronic storage media or to conduct a forensic examination of the electronic storage media;

n. records of or information about Internet Protocol addresses used by the electronic storage media;

o. records of or information about the electronic storage media's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses;

p. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as prints, slides, negatives, videotapes, motion pictures, or photocopies). This shall include records of telephone calls; names, telephone numbers, usernames, or other identifiers saved in address books, contacts lists and other directories; text messages and other stored communications;

subscriber and device information; voicemails or other audio recordings; videos; photographs; e-mails; internet browsing history; calendars; to-do lists; contact information; mapping and GPS information; data from "apps," including stored communications; reminders, alerts and notes; and any other information in the stored memory or accessed by the electronic features of the computer, electronic device, or other storage medium.

This warrant authorizes a review of records and information seized, copied or disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the ATF may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES DISTRICT COURT

for the

District of Arizona

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
GMC Savana U-Haul van bearing Arizona License Plate AL82438, at 529 W. 32nd Street, Yuma, AZ 85364

Case No. 22-3002MB

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*
See Attachment A

located in the _____ District of Arizona, there is now concealed *(identify the person or describe the property to be seized)*:
See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18 U.S.C. 922(a)(6)	Material False Statement During the Purchase of a Firearm

The application is based on these facts:
See attached Affidavit, incorporated by reference.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

GAYLE HELART Digitally signed by GAYLE HELART Date: 2022.12.31 22:38:58 -07'00'
Reviewed by Gayle L. Helart, AUSA

Kyle Dandoy
Applicant's signature

Kyle Dandoy, ATF Special Agent
Printed name and title

Sworn to and signed electronically.

Date: 12-31-22 @ 10:55 p.m.

Michael T. Morrissey
Judge's signature

City and state: Phoenix, Arizona

Michael T. Morrissey, United States Magistrate Judge
Printed name and title

ATTACHMENT A

Property to Be Searched

The vehicle is a white GMC Savana U-Haul van bearing Arizona License Plate AL82438, Vehicle Identification Number (VIN): 1GTW7AFPXN1247737, currently parked at *Cal-Ranch,* 529 W. 32nd Street Yuma, AZ 85364.

ATTACHMENT B

Property to be seized

1. Firearms, ammunition, magazines, cases, boxes, holsters, slings, gun pieces, gun cleaning items or kits, ammunition belts, original box packaging, targets, expended pieces of lead, and records, receipts, or other paperwork showing the purchase, storage, disposition, or dominion and control over firearms and ammunition;

2. Records, receipts, notes, ledgers, customer lists, invoices, and any other documentation related to the manufacture, importation, transportation, ordering, purchase, sale, or distribution of firearms;

3. Records relating to the receipt, transportation, deposit, transfer, or distribution of money, including but not limited to, direct deposit confirmations, wire transfers, money orders, cashier's checks, check stubs, PayPal or other electronic money transfer services, check or money order purchase receipts, account statements, and any other records reflecting the receipt, deposit, or transfer of money;

4. Safe deposit box keys, storage locker keys, safes, and related secure storage devices, and documents relating to the rental or ownership of such units;

5. Indicia of occupancy, residency, rental, ownership, or use of the Subject Premises and Vehicle found thereon during the execution of the warrant, including, utility and telephone bills, canceled envelopes, rental, purchase or lease agreements, identification documents, keys, records of real estate transactions, vehicle titles and registration, and vehicle maintenance records;

6. Cellular Phones (known as "electronic storage media");

7. Records evidencing ownership or use of electronic storage media, including sales receipts, registration records, and records of payment;

8. Any records and information found within the digital contents of any

electronic storage media seized from the Subject Premises, including:

a. all information related to the sale, purchase, receipt, shipping, importation, transportation, transfer, possession, or use of weapons and/or controlled substances;

b. all information related to buyers or sources of weapons and/or controlled substances (including names, addresses, telephone numbers, locations, or any other identifying information);

c. all bank records, checks, credit card bills, account information, or other financial records;

d. all information regarding the receipt, transfer, possession, transportation, or use of firearm proceeds;

e. any information recording schedule or travel;

f. evidence of who used, owned, or controlled the electronic storage media at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, correspondence, and phonebooks;

g. evidence indicating how and when the electronic storage media were accessed or used to determine the chronological context of electronic storage media access, use, and events relating to crime under investigation and to the electronic storage media user;

h. evidence indicating the electronic storage media user's state of mind as it relates to the crime under investigation;

i. evidence of the attachment to an electronic storage medium of another storage device or similar container for electronic evidence;

j. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the electronic storage media;

k. evidence of the times the electronic storage media were used;

l. passwords, encryption keys, and other access devices that may be necessary to access the electronic storage media;

m. documentation and manuals that may be necessary to access the electronic storage media or to conduct a forensic examination of the electronic storage media;

n. records of or information about Internet Protocol addresses used by the electronic storage media;

o. records of or information about the electronic storage media's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses;

p. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as prints, slides, negatives, videotapes, motion pictures, or photocopies). This shall include records of telephone calls; names, telephone numbers, usernames, or other identifiers saved in address books, contacts lists and other directories; text messages and other stored communications;

subscriber and device information; voicemails or other audio recordings; videos; photographs; e-mails; internet browsing history; calendars; to-do lists; contact information; mapping and GPS information; data from "apps," including stored communications; reminders, alerts and notes; and any other information in the stored memory or accessed by the electronic features of the computer, electronic device, or other storage medium.

This warrant authorizes a review of records and information seized, copied or disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the ATF may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

Your Affiant, Kyle Dandoy, being first duly sworn, hereby deposes and states as follows:

I. INTRODUCTION AND AGENT BACKGROUND

1. Your Affiant makes this Affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises located at **2730 S. 4th Avenue, Room #206, Yuma, AZ 85364** (Knights Inn motel) (hereinafter the "**Subject Premises**"), as further described in Attachment A of the Motel Room warrant, and a **white GMC Savana U-Haul van bearing Arizona License Plate AL82438, VIN 1GTW7AFPXN1247737 (hereafter "Subject Vehicle"),** as further described in Attachment A , (hereinafter the **"Vehicle"),** in order to search for and seize the items outlined in Attachment B, which represent evidence, fruits, and/or instrumentalities of the criminal violations further described below.

I am requesting this warrant to be executed during nighttime hours, 10:00 p.m. – 6:00 a.m. This investigation has covered a time period of two days, December 30-31, 2022. With respect to the Subject Premises, the room sought to be searched is a motel room at the Knights Inn which has been continuously watched by law enforcement with no one entering or exiting since approximately 5:30 p.m. on December 31, 2022. With respect to the Vehicle, it has been under constant surveillance by law enforcement since approximately 1:40 p.m. on December 31, 2022, as it is parked in a parking lot at a location separate from the Subject Premises. Both the Subject Premises (with other people having easy access such as employees) and Vehicle (moveable) may have firearms inside.

2. I am a Special Agent with The Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), and have been since May 2021. During my tenure as a Special Agent, I have completed approximately 500 hours of instruction at the Federal Law Enforcement

Training Center in Glynco, Georgia (FLETC). I also completed approximately 750 hours of Special Agent Basic Training (SABT) at FLETC.

3. Prior to my tenure as a Special Agent, I worked for the Yuma Police Department (YPD) from November 2011 to May of 2021. During my time at YPD, I conducted many investigations ranging from property crimes to shootings for approximately 6 years while working in a patrol capacity. I was also an instructor in various topics to include Driving, Firearms, High Risk Stops, etc. I also spent approximately 3 ½ years in the training unit before returning to patrol, where I continued to instruct and perform patrol duties, which included investigations.

4. The statements contained in this Affidavit are based on information derived from your Affiant's personal knowledge, training and experience; information obtained from the knowledge and observations of other sworn law enforcement officers, either directly or indirectly through their reports or affidavits; surveillance conducted by law enforcement officers; information provided by a confidential source; analysis of public records; analysis of social media information; analysis of telephone records; intercepted communications; and analysis of financial records.

5. Because this Affidavit is being submitted for the limited purpose of establishing probable cause for the requested warrant, I have not set forth all of the relevant facts known to law enforcement officers.

6. Based on the facts contained in this affidavit, there is probable cause to believe that Roberto PARTIDA has committed a violation of 18 U.S.C. § 922(a)(6), Material False Statement During the Purchase of a Firearm and evidence of such crimes will be found at **Subject Premises** and within the **Vehicle.**

II. PROBABLE CAUSE

7. On December 31, 2022, the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) was alerted by Cal-Ranch, a local Yuma Federal Firearms Licensee (FFL) of multiple firearm purchases made in cash by a male identifying himself as James Christopher Kohl (later determined to be Roberto PARTIDA). The FFL believed his drivers license to be fake. The Arizona Drivers License name used by the male was James Christopher Kohl with a date of birth XX/XX/1990 (full DOB known to me) and an Arizona Driver's License number of XXXXX0560 (full driver's license number known to me).

8. The FFL requested that I investigate the possible fake driver's license. I determined the photograph on the driver's license displaying James Christopher Kohl's name was not the same photograph according to the Arizona Department of Motor Vehicles (DMV) records.

9. I contacted several FFLs in Yuma County and learned PARTIDA purchased a total of nine (9) firearms on December 30-31, 2022.

10. Specifically, PARTIDA purchased two (2) firearms from *Sprague's Sports,* (one being a Taurus, 2-85629 Model, 38 Cal. Revolver S/N ACJ296952, and a second being a Glock G26 9 mm pistol S/N BYAD865).

11. PARTIDA purchased two (2) firearms from *Sportsman's Warehouse,(*both Springfield, Hellcat Model, 9mm pistols, S/N BB393192 and S/N BA581522).

12. PARTIDA purchased five (5) firearms from *Cal-Ranch.* Specifically, involving his purchases from *Cal-Ranch,* I was advised by *Cal-Ranch* that PARTIDA first purchased two (2) firearms on December 30, 2022, (both Springfield, Hellcat Model, 9 mm pistols, S/N BA254493 and S/N BB441482), and then returned to the store later on December 30, 2022, to purchase an additional two (2) firearms (Springfield Hellcat 9mm pistol S/N BB478583 and a Glock 26 9 mm pistol S/N AGPS365), however an employee

became suspicious of PARTIDA and delayed the purchase. On December 31, 2022, when PARTIDA returned to finalize the purchase of the third and fourth firearms, he purchased a fifth (an Altor Corp 9 mm pistol S/N AAB1942) for a total of five (5) purchased firearms from *Cal-Ranch*.

13. On December 31, 2022 when I became aware of this incident and started my investigation into PARTIDA's identity, I learned that PARTIDA contacted *Cal-Ranch* asking if his background was completed yet. An employee told PARTIDA he was still delayed.

14. Shortly after I learned of this information, the local police department was keeping a look out for a U-Haul van as I was told PARTIDA was driving a U-Haul van. The local police department spotted the U-Haul described as white GMC Savana U-Haul van bearing Arizona License Plate AL82438, Vehicle Identification Number (VIN): 1GTW7AFPXN1247737. I conducted surveillance on the vehicle and observed PARTIDA drive to Knights Inn motel, the **Subject Premises**, and stand by room #206.

15. The local police department inquired with the front desk and learned the renter of room #206 was a person using the name James Kohl (PARTIDA). Shortly after I witnessed PARTIDA at the **Subject Premises**, additional surveillance was conducted by other officers and PARTIDA was witnessed leaving the **Subject Premises.**

16. PARTIDA drove to *Cal-Ranch* and purchased the third and fourth firearms he had attempted to purchase on December 30, 2022, as PARTIDA called *Cal-Ranch* and asked again if his background was clear. PARTIDA was told he received his proceed status.

17. Upon PARTIDA purchasing the third and fourth firearms from Cal-Ranch, he also purchased a fifth, and agents contacted PARTIDA as he left the FFL and was approaching the U-Haul vehicle. Agents stopped PARTIDA and identified themselves.

18. I read PARTIDA his *Miranda* rights and he declined to talk. I advised PARTIDO that I would not ask him any questions about the gun purchases, however, I needed to identify him. He told me his name was Robert Partida, DOB XX/XX/1983 (full DOB known to me) with Social Security Number XXX/XX/2076 (full SSN known to me). PARTIDA possessed a fake driver's license with his photograph but in the name of James Christopher Kohl.

19. Based on my training and experience, I know Glock, Taurus, and Springfield firearms to be manufactured outside of the state of Arizona. Therefore, they would have needed to travel across state lines to be in Arizona.

Subject Premises and Vehicle

20. On December 31, 2022, around 5:30 in the evening, agents and local police began conducting surveillance at **Subject Premises**. As the writing of this warrant, no movement has been seen at the **Subject Premises. The Subject Vehicle** remains parked at Cal-Ranch and has been continuously observed and no one has come to the vehicle or left the vehicle since we contacted PARTIDA.

III. ITEMS TO BE SEIZED

21. Based upon the facts contained in this Affidavit, your Affiant submits there is probable cause to believe that the items listed in Attachment B will be found at the **Subject Premises**.

22. Based on my training, education, and experience, and discussions with other trained law enforcement personnel, along with information provided by sources of information and confidential sources, your Affiant knows the following:

A. It is common for persons involved in firearms trafficking to possess firearms and/or ammunition and to store those items inside their residences, vehicles, sheds, and storage units; to include, any such places easily accessible to them and/or under

their control. Unlike money and illegal drugs, firearms and ammunition (whether possessed legally or illegally) remain in the possession of individuals for much longer periods of time. Where money and illegal drugs are normally consumed, disposed of and/or moved within hours, days or weeks of acquisition, firearms and ammunition (unless previously used by the possessor in a violent act) are kept for weeks, months, years or a lifetime.

B. Documents and records related to the purchase of firearms, such as receipts, photographs, and ledgers, are also frequently stored in a purchaser's residence, also for long periods of time. Similarly, where there is indicia of firearms trafficking related to the purchase of firearms, I also know that other documents such as customer lists, buyer/seller lists, log books and contact information documents are also frequently found in a purchaser's residence.

C. It is common for there to be articles of personal property and documents on the premises or in the vehicles evidencing the identity of persons controlling the premises and vehicles.

D. It is common a tactic for individuals who cannot legally possess firearms to acquire them by using a person close to them (such as a spouse/romantic partner or other family member) who can otherwise legally purchase and possess firearms) to purchase firearms on their behalf. This practice of one person purchasing firearms on behalf of another while claiming to be the actual buyer or transferee is often referred to as "straw purchasing" a firearm.

E. Persons engaged in straw purchasing firearms will often purchase multiple firearms of the same or similar make and model. They will often pay in cash and use incorrect, old, or false addresses to conceal their actual residence and prevent law enforcement from tracing the firearms back to them. Firearms that have been

straw-purchased often are recovered by law enforcement during unrelated criminal investigations or at crime scenes within a relatively short time period, referred to as time-to-crime ("TTC").

F. Firearms traffickers often maintain paper and electronic records of their firearms trafficking for long periods of time and therefore are likely to be found at the **Subject Premises.**

G. Firearms traffickers commonly use computers, cellular telephones, and other electronic devices to communicate with other firearm traffickers and customers about firearm-related activities through the use of telephone calls, text messages, email, chat rooms, social media, and other internet and application-based communication forums. Moreover, firearm traffickers commonly use other capabilities of computers and electronic devices to further their firearm trafficking and money laundering activities. Therefore, evidence related to firearm trafficking activity and money laundering activity is likely to be found on electronic storage media found at the **Subject Premises**, as further described below.

H. In addition to items which may constitute evidence, fruits and/or instrumentalities of the crimes set forth in this Affidavit, your Affiant also requests permission to seize any articles tending to establish the identity of persons who have dominion and control over the **Subject Premises**, including rent receipts, utility bills, telephone bills, addressed mail, personal identification, keys, purchase receipts, sale receipts, photographs, vehicle pink slips, and vehicle registration.

IV. DIGITAL EVIDENCE STORED WITHIN ELECTRONIC STORAGE MEDIA

23. As described in Attachment B, this application seeks permission to search for records that might be found in or on the **Subject Premises**,or in the **Vehicle** in whatever

form they are found, including data stored on a computer, cellular telephone, tablet, or other media storage device, such as a thumb drive, CD-ROM, DVD, Blu Ray disk, memory card, or SIM card (hereafter collectively referred to as "electronic storage media"). Thus, the warrant applied for would authorize the seizure of all electronic storage media found in or on the **Subject Premises and Vehicle** and, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

24. *Probable cause.* Your Affiant submits that if electronic storage media are found in or on the **Subject Premises or in the Vehicle**, there is probable cause to believe records and information relevant to the criminal violations set forth in this Affidavit will be stored on such media, for at least the following reasons:

a. Your Affiant knows that when an individual uses certain electronic storage media, the electronic storage media may serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic storage media is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic storage media is also likely to be a storage medium for evidence of crime. From my training and experience, your Affiant believes that electronic storage media used to commit a crime of this type may contain: data that is evidence of how the electronic storage media was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

b. Based on my knowledge, training, and experience, your Affiant knows that electronic storage media contain electronically stored data, including, but not limited to, records related to communications made to or from the electronic storage media, such as the associated telephone numbers or account identifiers, the dates and times of the communications, and the content of stored text messages, e-mails, and other

communications; names and telephone numbers stored in electronic "address books;" photographs, videos, and audio files; stored dates, appointments, and other information on personal calendars; notes, documents, or text files; information that has been accessed and downloaded from the Internet; and global positioning system ("GPS") information.

c. Based on my knowledge, training, and experience, your Affiant knows that electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto an electronic storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on an electronic storage medium, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

d. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the electronic storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

25. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronic files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how the electronic storage media were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be found on any electronic storage media located in or on the **Subject Premises and Vehicle** because:

a. Data on a storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. File systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within electronic storage medium (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the owner. Further, activity on an electronic

storage medium can indicate how and when the storage medium was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on an electronic storage medium may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the existence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera) not previously identified. The geographic and timeline information described herein may either inculpate or exculpate the user of the electronic storage medium. Last, information stored within an electronic storage medium may provide relevant insight into the user's state of mind as it relates to the offense under investigation. For example, information within a computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on an electronic storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, electronic storage medium evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on one electronic storage medium is evidence may depend on other information stored on that or other storage media and the application of knowledge about how electronic storage media behave. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how an electronic storage medium was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

26. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on electronic storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. *The time required for an examination.* As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine electronic storage media to obtain evidence. Electronic storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. *Technical requirements.* Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the electronic storage media off-site and reviewing it in a controlled environment allows for a thorough examination with the proper tools and knowledge.

c. *Variety of forms of electronic media.* Records sought under this warrant could be stored in a variety of electronic storage media formats that may require off-site reviewing with specialized forensic tools.

27. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant your Affiant is applying for would permit seizing, imaging, or otherwise copying electronic storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media

or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

28. It is possible that the **Subject Premises and Vehicle** will contain electronic storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those electronic storage media, the warrant applied for would permit the seizure and review of those items as well.

V. CONCLUSION

29. Your Affiant submits there is probable cause to believe that the items listed in Attachment B, which constitute evidence, fruits, and/or instrumentalities of violations of 18 U.S.C. § 922(a)(6), Material False Statement During the Purchase of a Firearm is likely to be found at the **Subject Premises and Vehicle**, which is further described in Attachment A of the relevant Warrant.

30. I am requesting this warrant to be executed during nighttime hours, 10:00 p.m. – 6:00 a.m. With respect to the Subject Premises, the room sought to be searched is a motel room at the Knights Inn which has been continuously watched by law enforcement with no one entering or exiting since approximately 5:30 p.m. on December 31, 2022, but with the concern that others could gain access to it such as motel employees or other tenants. With respect to the Vehicle, it has been under constant surveillance by law enforcement since approximately 1:40 p.m. on December 31, 2022, as it is parked in a parking lot at a location separate from the Subject Premises, but the concern is that a vehicle is mobile and easy to burglarized if weapons are inside.

Kyle Dandoy

Special Agent Kyle Dandoy
The Bureau of Alcohol, Tobacco, Firearms and Explosives

Subscribed electronically and sworn to telephonically this 31 day of December 2022.

Michael T. Morrissey

HONORABLE MICHAEL T. MORRISSEY
United States Magistrate Judge